Summary

12 respondents
The trends indicate:
Most sites have a plan, and are not waiting to be told by DOE how to proceed.
Sites do not anticipate for DOE-HQ to provide or recommend a solution.
We need agreement on a set of policies
If there were a published set of guidelines, most would follow it.
Many are concerned they will deploy a system, then be told to change it.
There is strong agreement for the need to interoperate.
Want site autonomy for issue and revocation policies, and use of multiple keytypes.
Should be DOE guidance for when you must use strong tokens.
The complex should accept certificates issues by 3rd parties, but no site currently plans to use them.
DOE guidance sought on fields for x.509.
Primary uses of PKI are a) Originator verification, b) Encryption, c) Data integrity
Some sites think PKI is too much work for simple user verification and identification.

Discussions included a request that DOE issue a notice that if a site proceeds “with reasonable and industry-accepted care”, that DOE-HQ cannot force later changes.
DOE should make a statemwent whether they intend to act as root, or we will need to conduct site-by-site cross-certifications.

Each question is followed by the raw count of each answer value, then the mean, median, and mode

1	2	3	4	5	mean	median	mode

General guidance

0- don't know or doesn't matter 1- strongly disagree to 5-strongly agree

[ ] 1. A common minimum set of policies is necessary to achieve an effective complex-wide infrastructure.
0 0 1 6 6 4.4 4 4
[ ] 2a. This site needs external guidance on the necessary components for recognition of electronic copy as an original.
1 2 2 5 3 3.5 4 4
[ ] 2b. DOE should provide such guidance.
1 1 5 4 2 3.4 3 3
[ ] 2c. DOE should establish mandatory requirements for the acceptance of electronic copy as an original.
1 4 3 2 2 2.8 3 2
[ ] 3a. DOE should define a standard for establishing the minimum credentials and personal presence requirements when obtaining a signature certificate.
0 4 2 4 3 3.5 4 2
[ ] 3b. DOE should adopt a 3rd-party standard for minimum credentials and personal presence.
0 1 2 8 1 3.5 4 4
[ ] 3c. DOE should accept 3rd-party (national, international, or industry) standards in this area, and recognize certificates issued under those conditions.
0 0 1 7 4 3.9 4 4
[ ] 4a. This site wants guidance from DOE on when to use and not to use digital signature or encryption.
4 0 4 4 1 2.8 3 3
[ ] 4b. DOE should establish requirements on when to use and not to use digital signature or encryption.
3 3 2 4 1 2.8 3 4
[ ] 5. DOE should provide complex-wide policy on coupling (or allowing separate) keys for encryption and signature.
0 4 4 3 2 3.2 3 3
[ ] 6. This site needs to apply multiple signatures to a data item (document).
0 0 2 9 2 4.0 4 4
[ ] 7. This site understands the difference in definition and use between digital signatures and electronic approvals.
1 2 0 5 4 3.5 4 4
[ ] 8. This site's primary interest in PKI is for unclassified (including OUO and UCNI) purposes.
0 3 0 4 5 3.6 4 5
[ ] 9a. This site doesn't know how to proceed, and looks to DOE (HQ) for guidance.
5 1 4 1 1 2.2 2 1
[ ] 9b. This site wants to have input, but looks to the complex for guidance.
0 3 2 7 1 3.5 4 4
[ ] 9c. This site looks to industry for guidance.
0 1 2 8 1 3.5 4 4
[ ] 10. This site already has an established PKI for signature infrastructure, and is concerned that it will be disrupted by DOE guidance or policies.
2 5 2 2 0 2.0 2 2

Specific infrastructure elements

0- don't know or doesn't matter 1- strongly disagree to 5-strongly agree

[ ] 1a. Each site should determine its acceptable user token scenarios (e.g. hardware, floppies), key storage practices (e.g. key recovery, token lock-up), token encryption.

0 4 1 5 3 3.5 4 4

[ ] 1b. If there were a published policy from a DOE site for above, I would consider adopting it.

0 0 3 9 1 3.8 4 4

1c. DOE should regulate the following PKI elements for DOE transactions.

PKI elements:

[ ] -- key length

0 4 0 3 2 2.7 2 2

[ ] -- token acceptability

0 5 0 3 1 2.5 2 2

[ ] -- key storage practice

0 4 1 2 2 2.6 2 2

[ ] -- key recovery practice

0 5 1 1 2 2.5 2 2

[ ] -- encryption practice (including algorithms and implementation mechanisms)

0 5 0 2 2 2.5 2 2

1d. (Place an X by all that apply) My interpretation of the definition of "DOE transaction" includes the following possible definitions:

[ ] -- transactions between two DOE elements **(11 said yes)**

[ ] -- transactions between two DOE element or contractors **(8 said yes)**

[ ] -- transactions between a DOE element and another Federal agency **(6 said yes)**

[ ] -- any transaction involving a DOE element **(3 said yes)**

[ ] -- any transaction involving a DOE element or contractor **(4 said yes)**

[ ] -- any transaction in which DOE has a material interest involving a DOE element or contractor **(4 said yes)**

[ ] 2. Each site should determine their own expiration/ renewal cycle policy, and criteria for revocation.

0 2 3 6 1 3.2 4 4

[ ] 3. DOE should accept cross-certification for sites whose policies include delegation of signature through shared tokens or keyphrases.

1 2 2 4 2 2.8 3 4

[ ] 4a. DOE should determine a policy for mandatory use of "strong" tokens in certain cases (e.g. biometric or smart-card tokens in the case of $100-million procurements).

0 2 1 8 2 3.8 4 4

[ ] 4b. DOE should establish guidance for the use of strong tokens.

0 1 1 9 2 3.9 4 4

Certification and cross-certification

0- don't know or doesn't matter 1- strongly disagree to 5-strongly agree

[ ] 1. DOE should create and manage a DOE-wide Root (or centralized cross-certification), including minimum criteria for acceptance (who qualifies and how).
1 2 2 4 3 3.2 4 4
[ ] 2. DOE should have a criteria for assessing the stability (and intended longevity) of a site's a PKI before acceptance into the Root.
1 1 3 6 1 3.2 4 4
[ ] 3. DOE should accept the use of 3rd parties or certification companies for PKI practices audit/certification.
0 1 4 6 1 3.3 4 4
[ ] 4. DOE should accept 3rd party issuance and management of certificates and keys.
0 2 3 5 1 2.9 3 4
[ ] 5. This site plans to use keys/certificates for other uses (e.g. network sign-on, SHTTP, etc.).
0 1 2 6 1 3.1 4 4
[ ] 6a. DOE should provide guidance for the minimum contents of X.509 certificate fields.
0 0 2 8 2 3.7 4 4
[ ] 6b. DOE should define the required minimum contents of X.509 certificate fields for DOE transactions.
0 1 3 7 2 3.8 4 4
[ ] 7a. DOE should support the creation and maintenance of a list of minimum application interoperability requirements.
0 2 1 7 2 3.5 4 4
[ ] 7b. DOE should create and maintain a list of minimum application interoperability requirements.
0 4 2 4 2 3.1 3 2
[ ] 8a. Each site should set its own policy on recognition and use of multiple signature/encryption approaches (RSA, DSA, PGP,ssh, DES) and set guidelines for concurrent use.
1 4 2 5 1 3.1 3 4
[ ] 8b. The complex should support cross-certification of multiple signature/encryption approaches (RSA, DSA, PGP, ssh, DES).
0 3 1 6 2 3.3 4 4
[ ] 8c. DOE should support cross-certification of multiple signature/ encryption approaches that meet DOE performance standards.
0 1 1 8 2 3.6 4 4

About the responding site:

0- don't know or doesn't matter 1- strongly disagree to 5-strongly agree

[ ] 1. This site is waiting for somebody to tell us what to do so we can do it.
4 6 1 2 0 2.1 2 2
[ ] 2. This site is expecting DOE to create and manage a DOE-wide Root.
2 3 2 5 0 2.6 3 4
[ ] 3. This site plans to use an offsite 3rd party (eg VeriSign, US Postal) for issuing and management of site's certificates and keys. If so, who?
2 2 3 1 1 1.8 2 0
[ ] 4. My site is most concerned with policy matters regarding PKI and digital signature.
0 1 3 7 2 3.8 4 4
[ ] 5. My site is most concerend with technology and interoperabiltiy issues regarding PKI and digital signature.
0 1 3 8 1 3.7 4 4
6. Rank the following terms in order of relative importance (1= low importance, 5=high importance) that you anticipate solving (totally or in part) with digital signature or PKI.
[ ] Access control (what data or applications a user can reach)
2 1 2 3 4 3.2 4 5
[ ] Identification and Authentication (who is connecting or accessing the system or data)
0 0 2 3 8 4.5 5 5
[ ] Data confidentiality (encryption for storage or transmission)
2 0 2 1 8 4.0 5 5
[ ] Data Integrity (evidence of tampering)
0 0 4 2 7 4.2 5 5
[ ] Originator verification (who signed it)
0 0 1 3 9 4.6 5 5
[ ] Non-repudiation (prevents denial of having sent or seen the data)
0 2 2 4 5 3.9 4 5
[ ] Document approval (electronic approval)
0 0 3 4 6 4.2 4 5
[ ] Enterprise Security (consistent model for access control)
0 2 3 1 7 4.0 5 5